ISSN:2320-0790

An International Journal of Advanced Computer Technology

Finger-Vein Recognition Systems

A.Haritha Deepthi, S.Nithin Kalirajan, S.V.Thirupathi
Department of Information Technology, PSG Polytechnic College, Coimbatore, India

Abstract: As the Person's/Organization's Private information's are becoming very easy to access, the demand for a Simple, Convenient, Efficient, and a highly Securable Authentication System has been increased. In considering these requirements for data Protection, Biometrics, which uses human physiological or behavioral system for personal Identification has been found as a solution for these difficulties. However most of the biometric systems have high complexity in both time and space. So we are going to use a Real time Finger-Vein recognition System for authentication purposes. In this paper we had implemented the Finger Vein Recognition concept using MATLAB R2013a. The features used are Lacunarity Distance, Blanket Dimension distance. This has more accuracy when compared to conventional methods.

Keywords: Biometric, Finger vein Recognition, Lacunarity, SURF, MSER.

I. INTRODUCTION

Finger-Vein Recognition is a type of Biometric Authentication. Biometric identifiers are often categorized as physiological versus behavioral characteristics.

Physiological characteristics are related to the shape of the body. Examples fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and odour/scent.

Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to: typing rhythm, gait, and voice.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods.

II. BIOMETRICS

Biometrics (biometric authentication) refers to the identification of humans by their characteristics or traits. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals.

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. Jain *et al.* (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. **Universality** means that every person using a system should possess the trait. **Uniqueness** means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. **Permanence** relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. **Measurability** (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. **Performance** relates to the accuracy, speed, and robustness of technology used (see performance section for more details).**Acceptability** relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. **Circumvention** relates to the ease with which a trait might be imitated using an artifact or substitute.

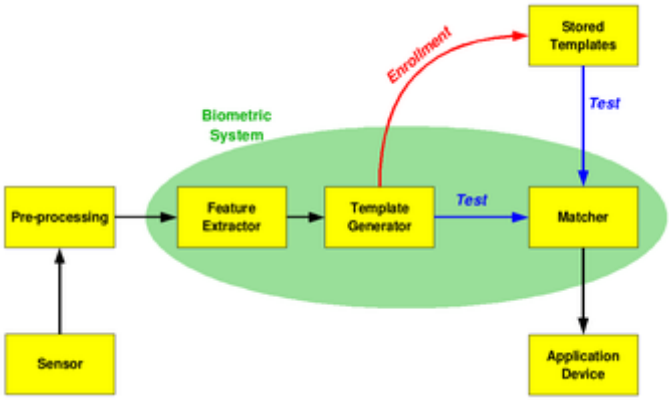

Fig2.1 Biometric System Diagram\

The basic block diagram of a biome in the following two modes. In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification.

In the first step, reference models for all the users are generated and stored in the model database.

In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold.

Third step is the testing step.

In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition ‘or for 'negative recognition' of the person The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

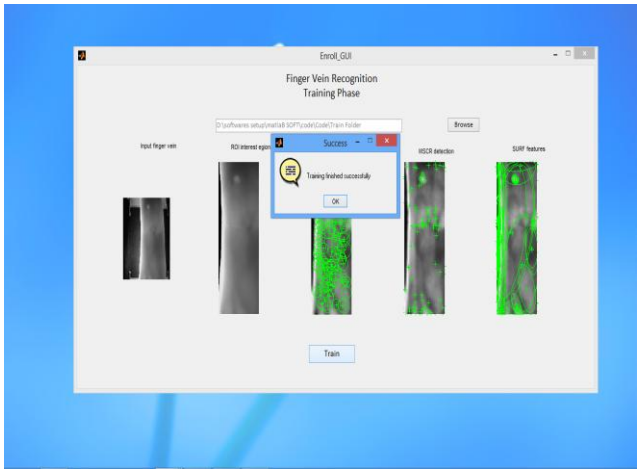

Fig 2.2 Enrollment

The first time an individual uses a biometric system is called *enrollment*. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption.

III. FINGER-VEIN RECOGNITION

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity.

Finger Vein ID is a biometric authentication system that matches the vascular pattern in an individual's finger to previously obtained data. Hitachi developed and patented a finger vein ID system in 2005. The technology is currently in use or development for a wide variety of applications, including credit card authentication, automobile security, employee time and attendance tracking, computer and network authentication, end point security and automated teller machines.

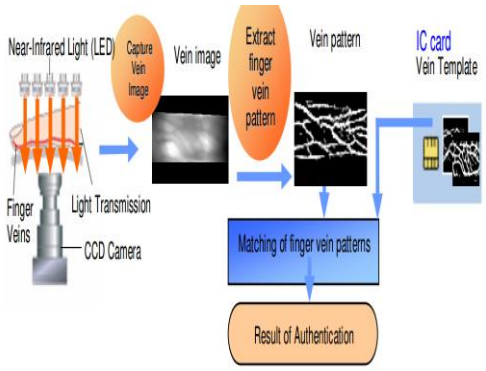

Fig3.1 Finger-Vein Recognition

To obtain the pattern for the database record, an individual inserts a finger into an attester terminal containing a near-infrared LED (light- emitting diode) light and a monochrome CCD (charge-coupled device) camera. The hemoglobin in the blood absorbs near-infrared LED light, which makes the vein system appear as a dark pattern of lines. The camera records the image and the raw data is digitized, certified and sent to a database of registered images. For authentication purposes, the finger is scanned as before and the data is sent to the database of registered images for comparison. The authentication process takes less than two seconds.

Fig 3.2 Testing Phase

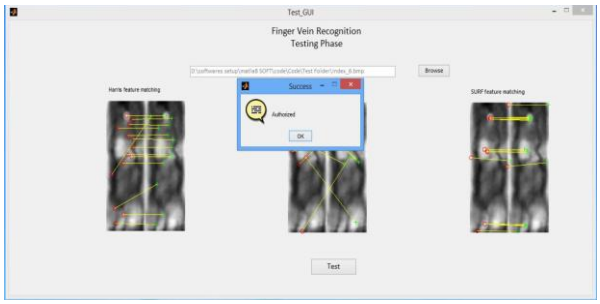

Fig 3.3 Authorized

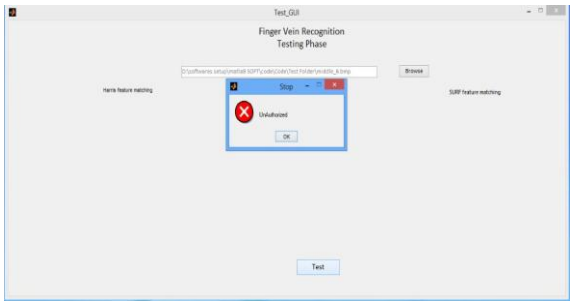

Fig 3.4 Unauthorized

Blood vessel patterns are unique to each individual, as are other biometric data such as fingerprints or the patterns of the iris. Unlike some biometric systems, blood vessel patterns are almost impossible to counterfeit because they are located beneath the skin's surface. Biometric systems based on fingerprints can be fooled with a dummy finger fitted with a copied fingerprint; voice and facial characteristic-based systems can be fooled by recordings and high-resolution images. The finger vein ID system is much harder to fool because it can only authenticate the finger of a living person.

IV. FEATURES

A. SURF

B. **SURF (Speeded Up Robust Features)** is a robust local feature detector, first presented by Herbert Bay et al. in 2006, that can be used in computer vision tasks like object recognition or 3D reconstruction. It is partly inspired by the SIFT descriptor. The standard version of SURF is several times faster than SIFT and claimed by its authors to be more robust against different image transformations than SIFT. SURF is based on sums of 2D Haar wavelet responses and makes an efficient use of images. It uses an integer approximation to the determinant of Hessian blob detector, which can be computed extremely quickly with an integral image (3 integer operations). For features, it uses the sum of the Haar wavelet response around the point of interest. Again, these can be computed with the aid of the integral image.

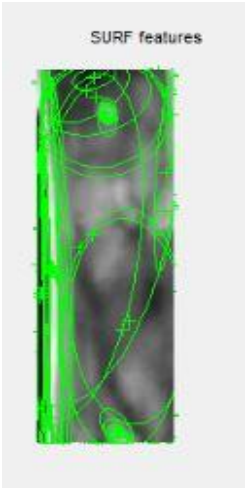

Fig 4.1 SURF

The task of finding correspondences between two images of the same scene or object is part of many computer vision applications. Camera calibration, 3D reconstruction, image registration, and object recognition are just a few. The search for discrete image correspondences – the goal of this work – can be divided into three main steps.

First, 'interest points' are selected at distinctive locations in the image, such as corners, blobs, and T-junctions. The most valuable property of an interest point detector is its repeatability, i.e. whether it reliably finds the same interest points under different viewing conditions.

Next, the neighborhood of every interest point is represented by a feature vector. This descriptor has to be distinctive and, at the same time, robust to noise, detection errors, and geometric and photometric deformations.

Finally, the descriptor vectors are matched between different images. The matching is often based on a distance between the vectors, e.g. the Mahalanobis or Euclidean distance. The dimension of the descriptor has a direct impact on the time this takes, and a lower number of dimensions is therefore desirable.

In our experiments on benchmark image sets as well as on a real object recognition application, the resulting detector and descriptor are not only faster, but also more distinctive and equally repeatable.

When working with local features, a first issue that needs to be settled is the required level of invariance. Clearly, this depends on the expected geometric and photometric deformations, which in turn are determined by the possible changes in viewing conditions. Here, we focus on scale and image rotation invariant detectors and descriptors. These seem to offer a good compromise between feature complexity and robustness to commonly occurring deformations. Skew, anisotropic scaling, and perspective effects are assumed to be second-order effects that are covered to some degree by the overall robustness of the descriptor.

As also claimed by Lowe, the additional complexity of full affine-invariant features often has a negative impact on

their robustness and does not pay off, unless really large viewpoint changes are to be expected. In some cases, even rotation invariance can be left out, resulting in a scale-invariant only version of our descriptor, which we refer to as 'upright SURF' (U-SURF). Indeed, in quite a few applications, like mobile robot navigation or visual tourist guiding, the camera often only rotates about the vertical axis. The benefit of avoiding the overkill of rotation invariance in such cases is not only increased speed, but also increased discriminative power. Concerning the photometric deformations, we assume a simple linear model with a scale factor and offset. Notice that our detector and descriptor don't use color.

C. LACUNARITY

Lacunarity, from the Latin lacuna meaning "gap" or "lake", is a specialized term in geometry referring to a measure of how patterns, especially fractals, fill space, where patterns having more or larger gaps generally have higher Lacunarity. Beyond being an intuitive measure of gappiness, Lacunarity can quantify additional features of patterns such as "rotational invariance" and more generally, heterogeneity. This is illustrated in Figure 1 showing three fractal patterns. When rotated 90°, the first two fairly homogeneous patterns do not appear to change, but the third more heterogeneous figure does change and has correspondingly higher Lacunarity. The earliest reference to the term in geometry is usually attributed to Mandelbrot, who, in 1983 or perhaps as early as 1977, introduced it as, in essence, an adjunct to fractal analysis. Lacunarity analysis is now used to characterize patterns in a wide variety of fields and has application in multi fractal analysis.

D. MSER

Maximally stable extreme regions (**MSER**) are used as a method of blob detection in images. This technique was proposed to find correspondences between image elements from two images with different viewpoints. This method of extracting a comprehensive number of corresponding image elements contributes to the wide-baseline matching, and it has led to better stereo matching and object recognition algorithms.

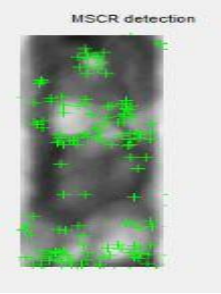

Fig 4.2 MSCR

Extreme Region $Q \subset D$ is a region such that either for all $p \in Q, q \in \partial Q : I(p) > I(q)$ (maximum intensity region) or for all $p \in Q, q \in \partial Q : I(p) < I(q)$ (minimum intensity region).

Maximally Stable Extreme Region

Let $Q_1, .., Q_{i-1}, Q_i, \cdots$ be a sequence of nested extreme regions ($Q_i \subset Q_{i+1}$). Extreme region Q_{i*} is maximally stable if and only if $q(i) = |Q_{i+\Delta} \setminus Q_{i-\Delta}|/|Q_i|$ has a local minimum at $i*$. (Here $|\cdot|$ denotes cardinality.) $\Delta \in S$ Is a parameter of the method.

The equation checks for regions that remain stable over a certain number of thresholds. If a region $Q_{i+\Delta}$ is not significantly larger than a region $Q_{i-\Delta}$, region Q_i is taken as a maximally stable region.

The concept more simply can be explained by thresholding. All the pixels below a given threshold are 'black' and all those above or equal are 'white'. If we are shown a sequence of threshold images I_t with frame t corresponding to threshold t, we would see first a white image, then 'black' spots corresponding to local intensity minima will appear then grow larger. These 'black' spots will eventually merge, until the whole image is black. The set of all connected components in the sequence is the set of all extreme regions. In that sense, the concept of MSER is linked to the one of component tree of the image. The component tree indeed provide an easy way for implementing MSER.

Extreme regions

Extreme regions in this context have two important properties that the set is closed under...

1. Continuous transformation of image coordinates. This means it is affine invariant and it doesn't matter if the image is warped or skewed.
2. Monotonic transformation of image intensities. The approach is of course sensitive to natural lighting effects as change of day light or moving shadows.

Advantages of MSER:

Because the regions are defined exclusively by the intensity function in the region and the outer border, this leads to many key characteristics of the regions which make them useful.

Over a large range of thresholds, the local binarization is stable in certain regions, and have the properties listed below.

- Invariance to affine transformation of image intensities
- Covariance to adjacency preserving (continuous)transformation $T : D \to D$ on the image domain
- Stability: only regions whose support is nearly the same over a range of thresholds is selected.
- Multi-scale detection without any smoothing involved, both fine and large structure is detected. Note however that detection of MSERs in a scale pyramid improves repeatability, and number of correspondences across scale changes.

- The set of all extreme regions can be enumerated in worst-case $O(n)$, where n is the number of pixels in the image.

E. HARRIS CORNER DETECTION

Harris corner detector is based on the local auto-correlation Function of a signal which measures the local changes of the Signal with patches shifted by a small amount in different directions.

Fig 4.3 HARRIS CORNER

V. CONCLUSION

The present study proposed an end-to-end finger-vein Recognition system based on the blanket dimension and Lacunarity implemented on a MATLAB platform. The proposed system includes a device for capturing finger-vein images, a method for ROI, and a novel method combining blanket dimension features and lacunarity features for recognition.We take the harris corner, MSCR, surf of the images from 6 fingers in the dataset were taken over long time interval by a prototype device we built. The experimental results showed that the method was 0.07%, significantly lower than those of other existing methods. Our system is suitable for application in laptops because of its relatively low computational complexity and low power consumption.

REFERENCES

[1] A. K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge", *Proceedings of the 17th International Conference onPattern Recognition (ICPR)*, vol. 2, pp. 935-942, 2004.

[2] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," *IEEE Transactionson Consumer Electronics*, vol 51, no. 2, pp. 545-551, May 2005.

[3] Y. Kim, J. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," *IEEE Transactions on Consumer Electronics*, vol.57, no.2, pp.756-762, May 2011.

[4] D. Wang , J. Li, and G. Memik, "User identification based on fingervein patterns for consumer electronics devices", *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, pp. 799-804, 2010.

[5] H. Lee, S. Lee, T. Kim, and Hyokyung Bahn, "Secure user identification for consumer electronics devices," *IEEE Transactions on Consumer 9+Electronics*, vol.54, no.4, pp.1798-1802, Nov. 2008.

[6] D. Mulyono and S. J. Horng, "A study of finger vein biometric for personal identification", *Proceedings of the International Symposium Biometrics and Security Technologies*, pp. 134-141, 2008.

[7]. Anil K. Jain, Patrick Flynn, and Arun A. Ross. Handbook of Biometrics. Springer-Verlag, USA, 2007.

[8]. W. O. Jungbluth. Knuckle print identification. Journal of Forensic Identification, 39:375–
380, 1989.

[9]. A. Kumar and C. Ravikanth. Personal authentication using finger knuckle surface. IEEE Transactions on Information Forensics and Security, 4(1):98 –110, 2009.

[10]. A. Kumar and Y. Zhou. Personal identification using finger knuckle orientation features. Electronics Letters, 45(20):1023 –1025, 2009.

[11]. David G. Lowe. Distinctive image features from scale-invariant keypoints. International
Journal of Computer Vision, 60:91–110, 2004.

[12]. Krystian Mikolajczyk and Cordelia Schmid. A performance evaluation of local descriptors.
IEEE Transaction Pattern Analysis Machine Intelligence, 27:1615–1630, October 2005.